by the applications level encryption and authentication software to encrypt files sent by the applications program before transmittal over ~~said open network.~~

31. (Amended) A method of carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising the steps of:

intercepting function calls and requests for service sent by an applications program in one of said client computers to a lower level set of communications drivers;

causing an applications level authentication and encryption program said one of said client computers to communicate with the server, generate [said] a session key, and use the session key generated by the applications level authentication and encryption program to encrypt files sent by the applications program before transmittal over said open network.---.

REMARKS

In parent U.S. Patent Application Ser. No. 08/917,341, claims 1, 5, 6, 16-19, 23, and 31 were rejected based on U.S. Patent No. 5,657,390 (Elgamel), and claims 2-4, 7-15, 20-22, 24-30, and 32-34 were allowed or indicated as being directed to allowable subject matter. In response, the claims indicated as allowable were re-written in independent form to include the limitations of the claim(s) from which they depended, with the remaining claims (including claims 16 and 17) being either already allowed or made dependent from allowed claims.

The present continuation application is directed solely to the rejected claims. The reason for presenting the rejected claims in this continuation application is that

Applicant does not believe that the Elgamel patent discloses or suggests the following concepts:

1. The concept of using "means for intercepting function calls...sent by an applications program on one of said client computers to a lower level set of communications drivers...and...means for causing an applications level authentication and encryption program...to...encrypt files sent *by the applications program...*," as claimed in claim 1;

2. A "shim" which intercepts the function calls and causes the applications level authentication and encryption program to communicate with the server and encrypt files as recited in claims 5 and 18; and

3. A method corresponding to the "means" of claim 1.

In Elgamel, the security protocol is implemented through the use of a secure sockets layer (SSL) which is bound to the applications program. As explained in col. 5, lines 17-35, the sockets layer "establishes a sockets connection with an application running on a remote computer and then performs a security handshake." This is in contrast to a conventional socket layer which just establishes the sockets connection and does not provide authentication and encryption.

The secure sockets layer disclosed in Elgamel thus *replaces* the conventional socket and is used by applications programs in the same manner as the conventional socket layer except that four additional function calls are added: "SSL_open, SSL_write, SSL_read, and SSL_close," as explained in col. 13, lines 1-57. In order to use the secure sockets layer to provide encryption services, an applications program must include the four function calls.

In contrast, the present invention does not necessarily replace any existing sockets or libraries, or require modification of existing applications programs.

Instead, it intercepts function calls used by the existing non-secure socket and diverts them to an applications level authentication and encryption program, which then uses the existing socket to establish communications with an authentication proxy server in order to perform the authentication and generate session keys. The applications program making the function call could just as well be making the function call to the ordinary socket rather than to the shim and is not affected by the authentication and encryption that is taking place, and as a result the present invention can be used with a wider range of applications programs and with a wider range of operating systems and socket connections than is possible with an Elgamel-type secure sockets layer. This provides the unique advantage of enabling direct peer-to-peer communications by any applications capable of using whatever socket programs are already installed in the client.

In other words, instead of just providing a socket that provides encryption services as in the Elgamel patent, the present invention inserts a shim between the sockets layer and applications programs that use the sockets layer. The shim diverts function calls to an applications level encryption and authentication program in a manner that is transparent to both the socket and the applications program, and the applications level encryption and authentication program initially directs communications to an authentication server in a manner which is also transparent to the applications program and sockets layer. There is no need to modify either the sockets layer or the applications program by adding new function calls as taught by Elgamel, and yet the invention provides a higher level of service and collateral functions for a wider variety of applications programs than is provided by the Elgamel secure sockets layer because, as claimed, authentication and generation of keys are carried out by communications between the applications level authentication and encryption program and a dedicated authentication proxy server.

As a result, it is believed that the claims presented in this continuation application are allowable over the Elgamel patent and all other references of record.

Early and favorable consideration of the amended claims on the merits is respectfully requested.

Respectfully submitted,

BENJAMIN E. URCIA
Registration Number 33,805

BACON & THOMAS

625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314
(703) 683-0500

Date: February 26, 1999

NWB-B:\53B.PRE